

ABSTRACT

Method for user identification and ascertainment of authenticity of parties in a telecommunication system comprising a telecommunication network; a source system connected to the telecommunication network; and a target system connected to the telecommunication network. According to the method, user identifiers and associated passwords are stored in the source system and in the target system; log-on into the source system is accomplished by entering a user identifier and a password corresponding to it; the user is identified in the source system; and a remote session to the target system is set up. In the invention, identical indexed encryption keys are generated in the source system and in the target system and the target communication between the source system and the target system is encrypted using an encryption key indicated by a given index and a kind of handshake operation is performed. By virtue of the handshake operation, the user can be identified with certainty. By using separate identification data, the source system and the target system can ascertain each other's authenticity.

10057376.0440